Approved: May 22, 2006

Council on Postsecondary Education
Data Policy—Institutional Data

Section 1: Purpose

This policy establishes the principles and practices related to collection, maintenance, use, analysis, and dissemination of data and information collected and maintained through the Kentucky Council on Postsecondary Education (CPE) comprehensive database system.

Section 2: Statutory Authority

KRS 164.020, KRS 164.095, and KRS 164.283

Section 3: Background

The CPE maintains and manages a unit record database containing public and private higher education institutional data used by the CPE for state and federal reporting, policy analysis, and decision-making. This database is referred to as the comprehensive database system.

The data and information collected through the comprehensive database system are used in support of improvements to instruction and to evaluate and measure performance within the system, all in support of postsecondary education reform. The data and information collected also is part of a comprehensive accountability system that the CPE is required to develop and maintain by KRS 164.020 and KRS 164.095.

The CPE protects all data and information in accordance with the Family Educational Rights and Privacy Act (FERPA) 20 U.S.C. § 1232g, et. seq. and applicable state laws. Where the data collected contain individual data on students, it is subject to both privacy and confidentiality procedures.

Section 4: Definitions

A. "Confidentiality" means how personally identifiable information collected by an authorized agency is protected and when consent by the individual is required.

B. "Council," "Council on Postsecondary Education," or "CPE" refers both to the agency established in KRS 164.011, to the staff of the agency employed pursuant to KRS 164.013, and to agency representatives who are employed by the CPE and who are under the direct control of the agency.

C. "Directory information" means information contained in an education record which would not generally be considered harmful or an invasion of privacy if disclosed to the public. The definition of directory information shall be specific to each institution.

D. "Education records" means those records directly related to a student and maintained by an educational agency or institution.

E. "Family Educational Rights and Privacy Act or FERPA" means the federal law codified at 20 U.S.C. 1232g and its implementing regulations found in 34 C.F.R. Part 99.

F. "Legitimate educational interest," for purposes of this policy, is an endeavor that furthers the understanding of educational practices, methods, and/or theory through formal, accepted research practice.

G. "Personally identifiable information" means information contained in an education record such as a personal identifier, characteristic, or other information that would make a student's identity easily traceable.

H. "Privacy" means the right of an individual to have personal information adequately protected to avoid the potential for substantial harm, embarrassment, inconvenience, or unfairness.

I. "Research" means a formal investigation designed to develop or contribute to general knowledge.

J. "State and local education authority" means an agency or other party with educational expertise and experience that is responsible for and authorized under state or local law to regulate, plan, coordinate, advise, supervise, or evaluate elementary, secondary, or postsecondary education programs, services, agencies, or institutions in the state.

K. "Third party" is a party other than the institution who provided the data to the CPE.

Section 5: Policy

A. General

1. This policy shall apply to all data and information created, collected, and maintained by or for the CPE, whether in electronic, paper, or other format.

2. The CPE is authorized by KRS 164.020(6) and (26) and KRS 164.095 to perform research on postsecondary education related issues, to maintain an accountability system, and to evaluate the performance of institutions in regard to the goals of the *Kentucky Postsecondary Education Improvement Act of 1997* and the strategic agenda.

3. Data collected and maintained by the CPE shall be managed in a manner that supports the improvement of education in Kentucky consistent with the goals of the *Kentucky Postsecondary Education Improvement Act of 1997* and the *Adult Education Act of 2000*. The CPE shall promote access to and dissemination of nonpersonally identifiable information that improves the education-related decisions of parents, teachers, administrators, policymakers, and educational stakeholders as well as the general public.

4. Where access to personally identifiable information is restricted by federal and state law, the information shall be processed (e.g., aggregated, summarized, or characterized) to provide access while meeting the requirements for restriction.

5. This policy will adhere to restrictions on the releases of personally identifiable information identified in the FERPA, 20 U.S.C. 1232g, and KRS 164.283.

6. The CPE shall ensure that data and information remain at all times under the direction and control of the CPE, that personally identifiable information is not disclosed to officials other than the CPE staff or contractors assigned to a project, and that all information is destroyed when there is no longer a need for the data for the purpose outlined.

7. Data access provisions may change if mandated by federal statute, state law, or administrative rules, where those changes are not in conflict with FERPA. The CPE may, at its discretion, propose changes in the data policy but the new rules shall not apply to data or information collected under the old policy unless proper notice has been given.

B. Security Requirements

1. Security includes measures to ensure that records are not lost, stolen, vandalized, illegally accessed, or otherwise rendered useless. Since the data are stored on computers, it is essential that there be a high level of protection that provides integrity and availability commensurate with the level of risk and magnitude of harm.

2. Data, copies of data, and all reports containing personally identifiable information shall be maintained in a secure environment to prevent unauthorized access. A secure environment includes any electronic media, personal computer, server, or network on which the data reside.

3. The CPE shall use encryption or other best practices when using personally identifiable information, and shall require institutions to use encryption or other best practices when transferring personally identifiable information to the CPE.

4. Private or confidential data on an individual shall not be created, collected, stored, used, maintained, or disseminated for any purpose other than for the stated purpose.

5. Disclosure in summary reports is designed to protect an individual's identity. The Council will establish a cell size standard for reporting of data when it is necessary to keep an individual from being identified.

6. Private or confidential data will not be released to the public, to a third party, nor to provider institutions except as provided for in 34 C.F.R. § 99.31 or to authorized staff of the postsecondary education institution who released the data to the CPE.

C. Requests by Individuals to Examine Their Personal Data

1. Upon request of individuals under Section 552a(f)(1) of the Privacy Act of 1974 or 34 CFR, Section 99.20 of FERPA to gain access to their records contained in the CPE comprehensive database system, the CPE will provide a copy of all or any portion in a comprehensible form and will consider requests, in consultation with the appropriate institution, to amend the record.

2. Individuals or groups requesting directory information contained in data files provided by institutions will be directed to the respective institution.

Certification: _____
Thomas D. Layzell

Original Approval: ____March 21, 2005_____

Amended: _____May 22, 2006_____